January 21, 2002 | Volume1, Issue 2

Homeland Defense Journal

"He is best secure from dangers who is on his guard even when he seems safe." —Syrus Publilius

Homeland Defense Journal, Inc. | Suite 1003 | 4301 Wilson Boulevard | Arlington, Virginia 22203
www.homelanddefensejournal.com | Phone: 703-807-2758 | Fax: 703-807-2758

The Winter Olympics:
'The Most Secure Place in the World'

Olympic Rings are "Rings of Steel"

Homeland Defense Journal

WASHINGTON — With a million visitors and 2,500 athletes from around the world converging on Salt Lake City next month, the 2002 Winter Olympics pose the first big test for the new Office of Homeland Security.

"This is going to be one of the most secure places in the world," Homeland Security Chief Tom Ridge said of the Olympic Village. "We have done everything humanly and technologically possible to prepare, to prevent, to detect, to disrupt and, in the very unlikely event that something were to occur, to respond to it in a meaningful way and very appropriate way."

The U.S. Secret Service is the lead agency for security at the Games, working in conjunction with the FBI and FEMA.

On the front line of defense will be the thousands of federal, state and local law enforcement officials with a show of force more conspicuous than at any event in the nation's history.

In addition, the Pentagon has provided 4,500 military servicemen, INS has committed more than 200 Border Patrol agents, EPA will provide support for state and local HazMat teams, the Bureau of Alcohol, Tobacco, and Firearms will be on hand for security checks, the CDC will have emergency response coordinators, lab scientists and other professionals on the ground, and HHS emergency medical teams and supplies are in place to respond to any public health threats.

All together, the security plans have involved 60 federal, state and local agencies to protect athletes and visitors at the Games – at 20 different venues spread out over a 6,000 square-mile area.

The price tag so far: More than $300 million in federal funds, about three times what the federal government spent on security for the 1996 summer games in Atlanta.

The Olympic Games have been a target for terrorists ever since 1972, when 11 athletes and officials were killed in an attack on the Olympic Village in Munich.

After the bombing at a public gathering at the Atlanta games, then-President Clinton established a task force to implement security for high-profile gatherings. This year, that role has been taken over by the Office of Homeland Security.

Officials said OHS has prepared for every possible contingency for the Olympics, which begin February 8th. They are working to secure critical infrastructures – including the power grid, air and water supplies around Salt Lake City – and guarding against cyberattacks.

The Utah Olympic Public Safety Command (UOPSC), has created an Internet-based system to allow law enforcement officers and other first responders from federal, state and local agencies to communicate directly and instantaneously. The system, created in conjunction with Science Applications International Corp., provides a single, secure communications channel for authorities to coordinate their efforts in the event of an emergency.

The skies will be closed to commercial air traffic when the Olympic torch arrives from its trip across the country, with AWACs surveillance planes patrolling above and fighter jets on

(continued on page 2)

Letters to the Editors

To the Editors:

If I were a terrorist, I would read this publication carefully. It provides a clear picture, through examples, of the massive efforts underway to prevent further penetration of America's immune system. And the pdf format is an excellent distribution method.

Please archive every issue!

— Scott Paine, Hydrologist
Newmont Mining Corporation
Carlin, Nevada

To the Editors:

I read the first issue of HDJ today. Among several articles of interest, I enjoyed MUNICIPAL REPORT: A Terrorist Attack at the Pentagon.

Before joining EPA in 1972, I spent four years in USAF as a ground radio operator. One of the basics of all Air Force communications was to always have available three systems of communications: the primary, and two backups. The primary was technically and maintenance-wise, the best performing and easiest to repair. The first back-up did just about everything the primary did but might offer fewer options or be less easy to fix. The second backup was usually some older gear with few features, still operative but no longer made, and with only a few replacement parts available.

You'd be surprised how many times that third system was employed and the missions it saved, not to mention the lives. Our emergency responders need to have at least three systems in place for all communications scenarios. As mentioned in the article, runners can be an acceptable back-up, as long as they can cover the distances without jeopardizing the mission.

— Connie Carr,
USEPA Region 3

Budget Battles and New Homeland Defense Initiatives Await Congress

Congress Returns from Winter Recess January 23rd

By Steven Kingsley
Homeland Defense Journal

WASHINGTON – President Bush is expected to ask Congress for an additional $15 billion in domestic security spending when lawmakers return to Washington from their winter recess on January 23.

The Pentagon, meanwhile, could get a $20 billion boost in the president's FY 2003 budget.

But as the prospect of a federal budget deficit grows, domestic programs could bear the brunt of new spending on homeland defense, leading to new budget battles on Capitol Hill.

"The rest of government will have to take second place," said OMB Director Mitch Daniels, noting that homeland defense must be the "number one priority" of government funding now.

Daniels defined priority homeland security projects as aviation security, public health, efforts to guard against bioterrorism, and aid to police and firefighters.

Among the homeland defense bills Congress left unfinished prior to adjournment last December is HR. 3525, the Enhanced Border Security and Visa Entry Reform Act.

The bill, which passed the House and is awaiting Senate action, calls for:

Funding for 200 additional INS inspectors and support staff

Increased funding for INS personnel training

(continued on page 2)

Cyber Attack: A Grave Threat to Power, Water, and Telecommunications

How Vulnerable Are We?

Congress is responding to fears of a cyber attack that could knock out power, drinking water, and telecommunications with a major boost for computer security research.

The Cyber Security Research and Development Act, legislation expected to pass Congress early this year, earmarks $880 million over five years to shore up computer security.

Funding would go to two federal agencies: The National Science Foundation (NIST) to fund university-based cybersecurity research centers and grants; and the National Institute of Standards and Technology (NIST) to provide grants for partnerships between academia and industry to work on computer security.

The legislation was developed in part because no federal agency currently is taking the lead in supporting cyber security research. Because private sector research typically targets short-term applications, the federal government has a key role in funding research to protect interdependent systems.

According to a new report by the Canadian Office of Critical Infrastructure Protection and Emergency Services, critical infrastructures in North America are at risk of cyberattacks that could cause a "domino effect," crippling electric power plants, gas plants and transportation systems.

"The Web sites will be safe, but the lights will be out, and water and oil won't flow. There have been vulnerability assessments done, and these important control systems have been shown to be vulnerable," said Joe Weiss, technical manager of the Enterprise Infrastructure Security Program at the Electric Power Research Institute.

"This is not in any way, shape, or form hypothetical," Weiss said in a recent issue of *Computer World*.

Last year, computer hackers gained access to the computer system that controls much of the flow of electricity across California and connects to the grid for the Western United States.

Recently, federal officials studied the ramifications of cyber attacks on critical infrastructures as part of security planning for the 2002 Winter Olympics. There, investigators found that the communications were the first thing to fail in any attack targeting a power grid.

"What was discovered is that if you have a prolonged power outage that goes on for several hours, your infrastructure starts to degrade. Power backup only lasts so long," said Paula Scalingi, director of the Department of Energy's Critical Infrastructure Protection Office, in an interview with CNN News.

Next affected are water systems, natural gas systems and gas-powered electric utilities.

"The infrastructure system providers didn't understand the interdependencies among their systems," Scalingi told CNN. "If you talk to state and local government and local utilities, they'll tell you they have great response plans. The problem is, they write them in isolation."

The Cyber Security Act (H.R. 3394) is sponsored by House Science Committee Chairman Sherwood Boehlert, R-N.Y., who said the federal government has made a "woefully inadequate" investment in computer security.

According to a committee background paper, no more than 75 researchers in the nation now have the experience to conduct cutting-edge research in computer security.

Private sector computer security experts still face barriers unrelated to funding. Intellectual property and digital copyright laws restrict computer research that uses copyrighted algorithms or breaches security mechanisms, including anti-copying protections.

Furthermore, anti-trust laws created to prevent collusion among competitors could prevent companies from working together to secure computer networks.

Companies involved in advising lawmakers on the legislation include Vericept, TruSecure Corp, Connected, Argus Systems Group, SpearHead Security Technologies and Top Layer Networks.

('Olympics' from page 1)

standby on the ground.

With more than 300 close-circuit surveillance cameras monitoring activity at every Olympic site, snipers and SWAT teams will patrol the grounds.

And Customs officials will screen every visitor against a federal "watch list" of suspected terrorists, and all visitors will go through one of 950 metal detectors. The security will be even tighter for athletes and officials: They must pass through biometric scanners before entering restricted areas.

This year more than any other, according to Mitt Romney of the Salt Lake Organizing Committee, the Olympic Rings are "rings of steel."

('Congress' from page 1)

- $150 million for new border security technology
- Systems to allow federal law enforcement and intelligence agencies to share data with federal and state agencies.

The bill is sponsored by Rep. Jim Sensenbrenner (R-WI) in the House. Sens. Ted Kennedy (D-MA) and Sen. Sam Brownback (R-KS) have introduced similar legislation in the Senate.

In other congressional news:

- Congress continues to grapple with mail processing problems following the anthrax mailings that shut down the Hart Senate Office building and disrupted mail deliveries to Capitol Hill. Because of off-site decontamination process, mail is still delayed at least two weeks. One solution under review involves scanning congressional mail at a secure site and then electronically sending it to the Hill. The *Roll Call* newspaper reports that a trial program could begin soon.

  According to an EPA estimate provided to Sen. Charles Grassley (R-IA), the cost of the anthrax cleanup at congressional buildings now exceeds $14 million.
- Some congressional Democrats are criticizing the Department of Transportation for a luggage screening program they say falls short of what federal law requires. While airlines began to institute tougher baggage policies on Friday January 18, many are simply matching bags to passengers rather than screening all bags for explosives as Congress intended.
- This decision amounts to a narrow interpretation of the statute and flouts the intent of a law designed to fundamentally change the air safety rules of our country," House Minority Leader Dick Gephardt said, criticizing DoT's decision to allow the passenger-bag match process as an alternative to actual inspections. "I'm afraid the secretary's announcement is little more than a perpetuation of the status quo."

  Transportation officials hope to have explosive screening devises in place at U.S. airports by December 31.

Taking the Disaster Out of Disaster Planning:

Real-Time Disaster Simulation Training Systems Utilized to Train First Responders

By George G. Groesbeck
Homeland Defense Journal

SARASOTA, FLA — It's been said that you cannot plan the response to a disaster without a disaster to plan with.

Emergency responders risk their lives every day responding to dangerous, unpredictable and often catastrophic incidents. Airplanes crash, chemicals spill, and trains derail. Timing is crucial. Lives are in the balance. Training plays a key role in how an incident is assessed, mitigated, and managed.

But state and local emergency plans are comprised of response criteria for disasters ranging from wildfires to terrorist attacks – and no two are alike.

As the United States – from the federal government to local communities – responds to potential terrorist threats, there is a new emphasis on jurisdictions working together to prepare disaster response and recovery plans.

"The loss of more than 340 firefighters and emergency personnel at the World Trade Center has hardened my resolve to see that local firefighters have the equipment and training they need, said FEMA Director Joe M. Allbaugh.

Increasingly, many agencies are using simulated disasters as a safe and effective means for emergency managers to practice their response to an emergency plan.

One such tool is the Advanced Disaster Management Simulator (ADMS™), manufactured by Environmental Tectonics Corp. of Southampton, PA.

ADMS™ is a computer-controlled training system that simulates a real-time disaster environment. It is designed to allow incident commanders to evaluate and re-evaluate their management strategies based on dynamic scenarios, including the likely behavior of people on the scene, vehicles, fires, explosions, chemicals, weather and other environment factors.

"In the simulation world, first responders can create whatever type of emergency and repeat different strategies, procedures, and events," according to ETC Sales Manager Ralph Huber.

The system also allows users to test and measure the aptitude of first responders, allowing them to identify problems and correct them before making a fatal mistake in the field.

Currently, the system is used by public safety agencies in Florida's Osceola, Orange, and Seminole counties, as well as the Orlando International Airport and the South Carolina State Emergency Management Agency.

System costs range from $30,000 to $4 million, depending on the complexity of simulation clients need. Funding for such systems will be available to public safety agencies through Homeland Security initiatives and grants.

For more information about the Advanced Disaster Management Simulator, contact Environmental Tectonics Corporation, 407-282-3378, or visit www.etcflorida.com

People in the News: John Magaw

Head of the Transportation Security Administration

Seasoned Professional Takes on Role as Undersecretary of Transportation for Security

The sight at our nation's airports and in the skies in the post-September 11th environment is one of armed National Guard troops, police, and sky marshals, as well as markedly increased screening procedures of passengers and luggage.

Following the September 11th tragedy, the U.S. Congress created the Transportation Security Administration (TSA) to focus on nationwide transportation security, and exercising his right to make recess appointments, President Bush installed John Magaw, a 26-year veteran of the United States Secret Service, to assume the new role of Undersecretary of Transportation for Security.

Magaw assumed the role on December 10th, bypassing a confirmation hearing in the Democrat-controlled Senate, which had failed to act on the Magaw appointment quickly.

"Given the importance of moving quickly to protect the public... and the upcoming deadlines in congressional legislation, the president thought it was too important to wait for Congress, and he was confident when Congress returns that Mr. Magaw would be confirmed," said White House spokesman Ari Fleischer.

As part of its mandate, the TSA will begin oversight of aviation security on February 18th, and Magaw will be responsible for setting standards for hiring and training of airport screeners, implementing standards for supervision of airport security employees, and developing threat plans for airline and airport security.

Magaw served as Director of the U.S. Secret Service in 1992, overseeing protective operations for the president and the first family. He headed the Bureau of Alcohol, Tobacco and Firearms from 1993 to 1999. He currently is acting executive director of the Office of National Preparedness at the Federal Emergency Management Agency.

HDJ AGENCY PROFILE: THE GENERAL SERVICES ADMINISTRATION

Homeland Defense Functions

The General Services Administration organizes homeland defense operations under the Federal Technology Service (FTS). http://www.fts.gsa.gov/

Divisions include:

Office of Information Assurance and Critical Infrastructure Protection

Assistant Commissioner Sallie McDonald 202-708-7000
sallie.mcdonald@gsa.gov
Contingency Planning Director Thomas E. Sellers 202-306-6751
thomas.sellers@gsa.gov

Federal Computer Incident Response Center

Director Lawrence C. Hale 202-708-5481
lawrence.hale@gsa.gov
Technical Director David L. Jarrell 202-708-5608
david.jarrell@gsa.gov

Center for Information Security Services

Director Melanie Lewis 202-708-6679
melanie.lewis@gsa.gov
Business Development Directors:
Douglas Campbell 202-708-7301
michael.campbell@gsa.gov
Kathleen Robinson 202-708-7303
kathy.robinson@gsa.gov

Office of the Federal Protective Service

Assistant Commissioner Richard Yamamoto 202-501-0907
richard.yamamoto@gsa.gov
Criminal Intelligence & Investigations Director
Larry Phelps 202-501-0793
larry.phelps@gsa.gov
Security & Technical Division Director Melvin Basye
202-501-0193
melvin.basye@gsa.gov

GSA Homeland Security Initiatives:

SAFEGUARD

The SAFEGUARD program assists federal agencies in implementing critical infrastructure protection plans.

The SAFEGUARD program provides services and products in conjunction with private industry to guard against "emerging unconventional threats," including physical and cyber attacks on critical infrastructures.

Services include security training, exercises and simulation; risk management; information assurance and emergency preparedness.

Industry partners include Booz, Allen & Hamilton, Electronic Data Systems Corp, Computer Sciences Corp., Collins Consulting Group, Lockheed Martin Corp., Telos Corp., Litton/PRC, Inc., CACI Intl, KPMG Consulting, UNISYS Corp., TRW Inc., and DynCorp Information Systems.

ENIGMA

ENIGMA is a program to assess potential cyber vulnerabilities and exposure to attack.

Initiated in May 2000 and now the federal standard for conducting computer assessments, ENIGMA uses INFOSEC Assessment Methodology (IAM) developed by the National Security Agency.

The U.S. Commerce Department was the first federal department to use ENIGMA in support of its Automated Export System.

When fully implemented, ENIGMA will be used for security planning, risk assessment, contingency planning, certification, accreditation, and information assurance security education and training.

DOING BUSINESS WITH THE GSA:

A vendor can only become a schedule contractor with the GSA in response to a specific solicitation. For more information, see: http://pub.fss.gsa.gov/sched/do_biz.cfm.

NEWSBRIEFS (HDJ Weekly Feature)

"Blackberry" Handhelds In Use at Logan … Bag-Matching Screening on U.S. Flights …Protection Urged for GPS Satellite System … Cockpit Door Security Standards Issued … SmartVisas ... the Army's SmarTruck …Chemresistor Sensors

Blackberries Offer New Law-Enforcement Tool for the Men and Women in Blue

A wireless tool that is the must-have accessory of IT workers and mobile professionals has been drafted into the campaign against terrorism.

Logan International Airport this month began testing the Blackberry to give law enforcement officers an instant, secure link to criminal databases.

Manufactured by Research in Motion, the Blackberry has been modified with software from Aether Systems to send and deliver encrypted data from state and federal databases.

With the device, aviation security officers can do instant background checks on air travelers and monitor the FBI list of suspected terrorists. Officers armed with Blackberries can communicate in real time with other officers – silently, instantly and without involving dispatch.

The device has other practical uses as well. According to the New England Law Enforcement Management Institute, patrols at Logan have used their Blackberries to identify stolen cars in the airport's parking lots.

Aether Systems supplied the devices with their PocketBlue software to Logan's security forces for free last year after the September 11th hijackers boarded the two doomed flights at the Boston airport. Aether said other municipal airports are considering testing the system as well.

The PocketBlue technology is also being used by law enforcement agencies in several regions, including California, Florida, Minnesota, Ohio and the Washington, D.C. metropolitan area.

Driver's Licenses: The New National ID Card?

State motor vehicle officials have asked Congress for up to $100 million to create a national database to store identity information on anyone who holds or applies for a driver's license.

Noting that driver's licenses have become the "de facto" national identification card, the American Association of Motor Vehicle Administrators called for the implementation of high-tech driver's licenses that use computer chips or biometric technology to store data.

The proposal, one of many Congress is considering to create a national identification system in the wake of the September 11th terrorist attacks, would require a federal initiative to link state motor vehicle databases, reform licensing procedures and replace tens of millions of driver's licenses nationwide.

The U.S. Department of Transportation already has begun work with individual states to create "smart" driver's licenses with driver information stored in a national database. Such information could eventually be passed to FBI, INS and other federal databases.

Currently, 26 states use a bar code on driver's licenses that stores some personal data, while nine states already use biometric technology.

Officials said weak licensing procedures provide a loophole through which foreign visitors – even those with expired travel visas – obtain identification cards. Federal authorities have determined that several of the September 11th hijackers used false identities and obtained driver's licenses illegally.

States currently require only a Social Security card and birth certificate – both of which can easily be forged – as proof of identity.

Airport Authorities Begin Screening Luggage on U.S. Domestic Flights

Just barely meeting the federal deadline of January 18th, U.S. Airlines have begun matching checked luggage to passengers on all domestic flights, under a system required by a new aviation security law.

But the system will be phased in gradually to address concerns about potential delays and operational problems.

Initially, bags will be matched to passengers on all originating flights, but not on connections.

Under the bag-matching process, long a standard on international flights, luggage must be removed from a plane if the passenger who checked it does not board the flight.

Some airports plan to instead begin implementing other baggage security measures, including screening bags for explosives. Bomb-detection technology is considered the most effective security measure, although it is expensive and time consuming. Federal aviation security law mandates that all airports use bomb-detecting x-ray machines by the end of 2002.

New Federal Standards Issued for Cockpit Door Security

The Federal Aviation Administration has issued new standards requiring U.S. airlines to install new cockpit doors that are resistant to gunshots or physical force.

Airlines have 18 months, until April 2003, to put new doors on nearly 6,000 planes in their fleets. The rules apply to all commercial passenger planes with 20 or more seats and all cargo planes with cockpit doors.

The new standards replace temporary security measures installed after the September 11th hijackings.

The rules, issued January 11th, require that the cockpit be locked at all times during flights, with doors designed to be unlocked only from the inside. The rules also mandate that only flight crewmembers have access to cockpit keys, tightening current standards that allow senior flight attendants to carry keys.

The standards do not, however, require airlines to make their cockpit doors blast-resistant, although aircraft manufacturers are working to develop doors that resist explosives.

The FAA estimates that the heavier, secure doors could cost as much as $17,000 per plane, with a total cost to the airline industry exceeding $120 million over 10 years, including the cost of increased fuel consumption.

A federal program that sets aside $100 million for aviation security upgrades will help carriers finance the project.

Several airlines have already begun installing the reinforced doors, including JetBlue, and companies that manufacture secure cockpit doors include TTF Aerospace of Washington and Galaxy Scientific of New Jersey.

Terrorism Response Training Video Available to First Responders

The FEMA X office in Bothell, Washington has developed a terrorism response training video and CD-ROM, available to local governments, fire, police and emergency departments. The video was produced from excerpts from the Pacific Northwest Terrorism Workshop, which brought together more than 100 federal, state and local government planners.

Copies are available by contacting FEMA's June Uson at (425) 487-4634.

CDC Aims to Arm Public Health Authorities with High-Speed Internet Access

In response to concerns that public health authorities will be unable to communicate in the face of a bioterrorist attack, the Centers for Disease Control and Prevention is launching an initiative to ensure that all state and county health departments have high-speed Internet access.

The effort comes in the wake of a CDC report concluding that the nation's counties may be seriously hampered in their efforts to communicate over the Internet in the case of a major terrorist attack.

The CDC report reveals that nearly half of the nation's 3,000 local health departments lack high-speed Internet access and cannot receive broadcast messages crucial to disaster response and recovery. Some public health laboratories – often the first to detect a dangerous new pathogen – still report lab test results by conventional mail, with lag times of up to 10-14 days. During the anthrax scare, several state public health departments were forced to coordinate their response by phone and fax, making it impossible to have an integrated response.

One of the lessons of the September 11th attacks is that federal, state

NEWSBRIEFS (continued)

and local authorities must be able to communicate and share information quickly and seamlessly. High-speed Internet communications are crucial to this process, according to Rep. Tom Davis (R-VA), chairman of the House Government Reform Subcommittee on Technology.

The CDC is offering grants to states to improve their public health communications systems. One such project links local, state and federal agencies with community health authorities and health care facilities.

The program is part of the Health Alert Network (HAN), an initiative led by the CDC in partnership with the National Association of County and City Health Officials, the Association of State and Territorial Health Officials, and other health organizations.

The Bush administration has requested an additional $40 million for HAN through the Emergency Response Fund.

"SmartVisas" Proposed for Border and Immigration Security

The Federal government is rapidly moving toward implementing tough new standards that would require that tamper-resistant passports and the use of biometrics, including face-recognition technology and fingerprint scans, at entry-exit points in airports and at U.S. borders.

One provision in the counter terrorism package signed into law last year called for digitized fingerprints to be included on an identification card required to enter the United States.

Under other legislation now under consideration on Capitol Hill, U.S. entry points would use machine-readable "Smartvisas" to screen foreign nationals seeking entry.

The market potential for "smart" identification technology in border control and immigration is immense. In 2000, the State Department issued more than 7 million U.S. passports and 6.5 million visas. The INS, meanwhile, conducted more than 500 million inspections at air, land and sea ports of entry.

Panel Urges Pentagon to Protect the Global Positioning System

A distinguished task force of anti-terrorism experts recommends in a new report that President Bush designate the Global Positioning System (GPS) a critical national infrastructure and assign the Pentagon to protect it.

"The GPS satellite network is an enabling system for other infrastructure systems that are vital to the nation's security . . . but has not been designated as a vital national asset," according to "Defending the American Homeland," a report by the Heritage Foundation Task Force on Homeland Security.

GPS, a space-based constellation of orbiting satellites developed by the Department of Defense, supply navigation for military and commercial uses. These include the telecommunications industry, the financial sector and the national electric grid.

The 24 GPS satellites are now unprotected in space. The system is also vulnerable, the Task Force said, because it uses a very low-power signal that can be corrupted or interrupted.

According to the report, Russia is "actively marketing" handheld GPS jamming equipment that can block receiving equipment for 120 miles. The system also is vulnerable to ballistic missile attack.

The Task Force also recommended that the Defense Department modify GPS satellites to include more robust signals and launch additional satellites to "augment the fragile constellation currently in operation."

The Heritage Foundation task force is chaired by Ambassador L. Paul Bremer, CEO of Marsh Crisis Consulting and chairman of the National Commission on Terrorism under Ronald Reagan, and former Attorney General Edwin Meese.

High-Tech Trucks Developed as Tool Against Terrorism

One new weapon in the war against terrorism has four wheels and looks like a pickup truck.

The National Automotive Center, the U.S. Army's vehicle research unit, is developing a multipurpose military vehicle that could also be sold as a rugged truck for civilians.

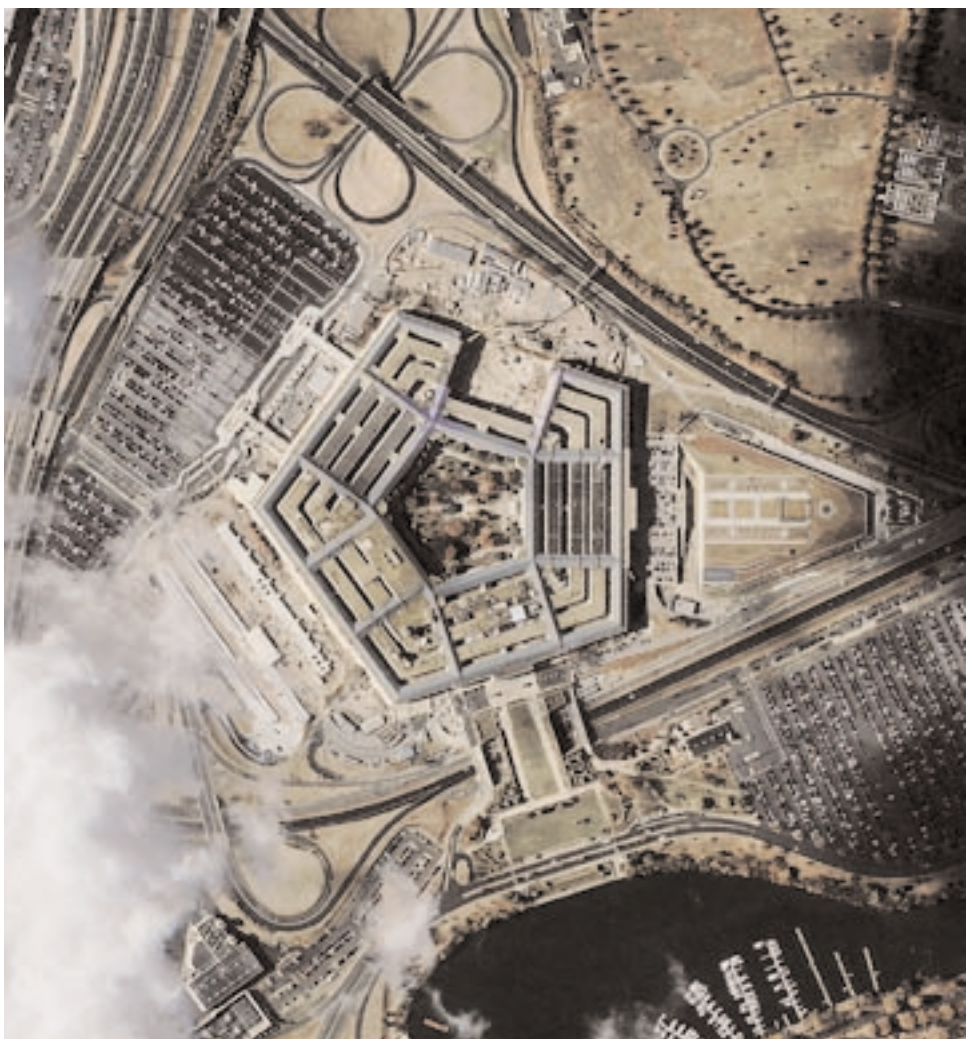
The "SmarTruck" features bulletproof armor, a fingerprint identification system, a night vision system and cutting-edge "countermeasure" features including a remote control weapon station, electrified door handles, blinding lights, smoke screens and a device that spews tacks from the rear of the vehicle.

Built by MSX International, the vehicle is designed with homeland security in mind. In addition to operating over rugged terrain, enhanced versions of the SmarTruck could protect occupants from chemical or biological attack.

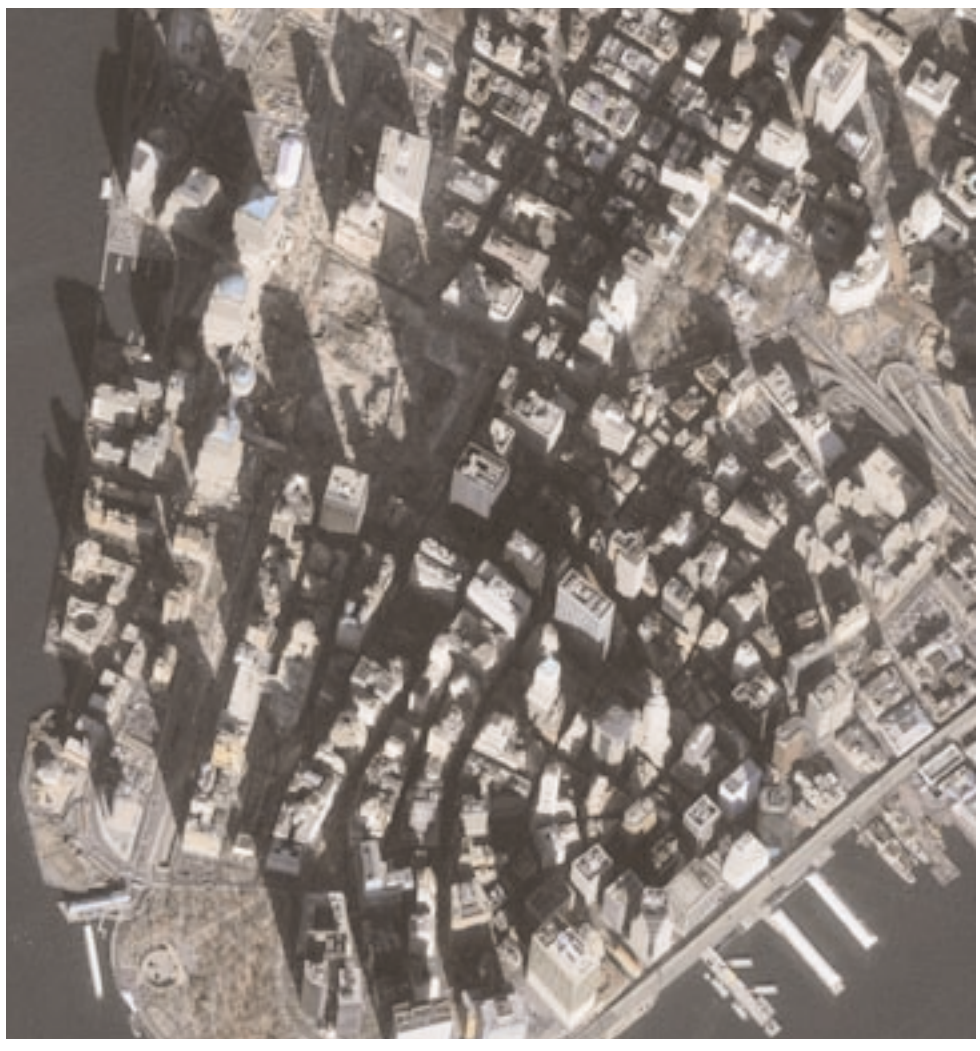
A prototype of the vehicle was on display at the North American International Auto Show in Detroit earlier this month, although the final product could take more than a year to complete.

"The concept is very agile, very chameleon-like," project engineer GerMaine Fuller told *The Washington Times.* "The vision was to have something that the military could use as well as other law enforcement agencies - but even for private security types of purposes, obviously without all of the features."

The NAC is part of the U.S. Army Tank-automotive and Armaments Command, or TACOM, which works in conjunction with U.S. automakers to develop new vehicular technology for defense and commercial use.



A view of the Pentagon from 423 miles above earth.



A view of the World Trade Center Site, December 2001

Satellite Imagery by Space Imaging, **www.spaceimageing.com**

Space Imaging is providing the world's first high-resolution commercial imaging products from the IKONOS satellite. Satellite image maps like this can be used by first responders and other emergency service planners, as well as for risk management and disaster assessment.

NEWSBRIEFS (continued)

New Sensors Can Monitor Air, Water for Chemical Contamination

New miniature sensors developed by Sandia National Laboratories could continually monitor air and water for agents of chemical and biological warfare.

The system is designed to detect potentially harmful organic compounds on site and transmit data to a remote computer, negating the need for sample collections and allowing for lower-cost monitoring and the nation's air and water supplies.

The technology, which is expected to be available for commercial use within one to three years, can also be used to monitor chemical spills, underground storage tanks and chemical waste dumps.

The sensors, also known as chemresistors, can detect aromatic hydrocarbons, chlorinated solvents, alcohols, ketone, and nerve gas agents, according to Sandia researchers.

The sensors are manufactured by mixing a commercial polymer with conductive carbon particles, producing a solvent which is then applied to electrodes on a circuit. As compounds absorb, the polymers swell and enable researchers to monitor and measure the change.

Packaged in small, waterproof housing, the sensors are covered by a Gore-Tex membrane that allows vapors to penetrate.

Sandia is also working with the Environmental Protection Agency and the American Water Works Association Research Foundation to train water utilities to analyze water supplies for dangerous compounds and prevent widespread contamination.

Government Agencies Speed Plans to Protect Databases

The U.S. Customs Service is among many federal agencies now accelerating plans to establish computer backup facilities to access data in the event of an attack or other emergency.

According to *Federal Computer Week*, the Customs Commercial Recovery Services program is awarding contracts to build a primary backup facility at least 20 miles from the agency's Springfield, Va., data center, as well as another facility at least 350 miles away.

Many federal agencies do not now have "operational" disaster recovery plans, the GSA's disaster recovery manager David Krohmal told *FCW,* but are now "ratcheting up" their plans in the wake of September 11th.

The Internal Revenue Service is also mounting an extensive effort to establish backup systems. Of the $16 million the IRS received in anti-terrorism funding, $13.5 million is earmarked for a computer recovery system.

Among the companies now working with the federal agencies on backup and recovery efforts are IBM Global Services, SunGard and Comdisco Inc.

Computer Simulation Used to Help Plan for Terrorist Attacks

The federal government will use computer simulation to assess the impact of possible terrorist attacks on the nation's critical infrastructure.

Scientists working with the National Infrastructure Simulation and Analysis Center will be joining the Office of Homeland Security to devise computer-simulated attacks on airlines, railways, energy pipelines and telecommunications systems to identify vulnerabilities, develop disaster assessment and recovery plans.

The modeling technology, previously employed to help guide urban planners, is being developed by NISAC scientists recruited from the Los Alamos National Laboratory to join Tom Ridge's homeland security team at the White House.

As an assessment tool, the NISAC can also be used to simulate the nation's computer networks and telecommunications systems.

The system will help officials determine the broad ramifications of attacks not now understood. Last summer, for example, a fire in a train tunnel in Baltimore affected Internet service in Chicago because the backbone of the high-speed network ran through the tunnel.

The NISAC was established as part of the Critical Infrastructures Protection Act of 2001 to "serve as a source of national competence to address critical infrastructure protection and continuity through support for activities related to counter terrorism, threat assessment, and risk mitigation."

In December, Congress appropriated $20 million for the NISAC as part of the Defense Department's anti-terrorism initiatives.

New Product Screens Mail for Biohazards at a Rate of 40,000 Pieces Per Hour

A new system developed by Lockheed Martin Corp. is capable of screening mail for biological hazards, including anthrax, by analyzing the air around mail sorting equipment.

BioMail Solutions can detect micron-size particles in the air with a system able to process as much as 40,000 pieces of mail per hour. Mail will travel on a high-speed conveyor belt through screening machines that are designed to shut down when a biohazard is detected.

Lockheed hopes to market BioMail to the government, corporations, universities and health care facilities.

In the wake of the anthrax attacks that killed five people last fall, the U.S. Postal Service has requested more than $5 billion to guard against biohazards sent through the mail.

Lockheed is also involved with Sandia National Laboratories in the development of a decontamination foam that kills anthrax spores.

HDJ Book Review: Public Health Law: Power—Duty—Restraint

By Lawrence O. Gostin, University of California Press

By Captain Elliott Grollman
Special to Homeland Defense Journal

When I first started in law enforcement many years ago, there were many areas of criminal law that I had to learn and keep up with: Arrest, search and seizure, authority and jurisdiction, to name a few. As new technology changed our society, that same technology created new opportunities for criminal activity; criminal activity for which many laws had not been passed yet or even considered.

Who would have thought that we would now have to deal with cybercrime dealing with identity theft, fraud, child porn and recipes for pipe bombs posted on the Internet?

Weapons of Mass Destruction pose another area new to the law enforcement field, specifically nuclear, chemical and biological terrorism. This new threat brings entirely new challenges involving response, training, and capabilities greater than anything law enforcement ever faced.

As a law enforcement official who has some responsibility in this area, I am always looking for ways to meet these challenges. *Public Health Law,* by Lawrence O. Gostin, may help shed light on this area.

Gostin, a professor of law at Georgetown University and co-director of the Georgetown/John Hopkins Program on Law and Public Health, examines a broad range of these new threats.

In his new book, Gostin reviews the conceptual foundation of public health law and offers a systematic evaluation of public health regulation.

Gostin also reviews conflicts between public health and civil liberties, examining issues relating to personal privacy, freedom of expression, immunization and testing, quarantine, regulatory powers and tort law.

Law enforcement officers can learn much from Gostin's analysis of public health practices as they concern personal control, forced quarantine, compulsory medical treatment and hospitalization and the criminal prosecution of those who willfully expose others to infection and disease.

While his book is not geared to all law enforcement officers, it is particularly relevant to public health authorities and other first responders who may be on the front line in the event of a terrorist attack.

The time to read it is now, before the worst can happen.

(*Captain Grollman is currently serving as the Chairman of the Law Enforcement Working Group on WMD at the Washington Metro Council of Governments.*)

AROUND THE STATES

Reserve and National Guard Preparedness … First Responders … "Crypto Card" Technology … Anthrax Vaccine Update

ALABAMA

Alabama leads the nation in activating part-time troops for the fight against terrorism. Since September 11th, Alabama has activated 2,412 Army Reserve and National Guard troops, more than Texas and Florida combined.

With a long history of military service, Alabama has traditionally had a strong National Guard force – the largest in the country prior to the defense cuts that followed the Gulf War.

ALASKA

Governor Tony Knowles has launched a two-year, $100 million homeland security initiative to secure the state's critical infrastructures, protect public health and train first responders to deal with the new threats of terrorism.

"Make no mistake - America is at war. Nearly everyday we receive new reports of potential terrorist acts - nuclear, chemical, biological, radiological - which until September 11th had been only the stuff of science fiction," Knowles said. "In addition to securing our own population, Alaska is uniquely positioned to respond to attacks elsewhere, given our geographic proximity to the Lower 48, Europe and Asia."

The effort, led by Department of Military and Veterans Affairs Commissioner Phil Oates, creates an Alaska Office of Homeland Security and funds additional law enforcement and public safety officers and increased security procedures.

"There is an increased price of freedom in this new era of terrorism," Knowles said, seeking $40 million in federal funds, $40 million in state funds, and $15 million from other sources.

CALIFORNIA

In his 2002 State of the State address, California Governor Gray Davis said "no state has done more than California to protect its citizens and vital assets since the terrorist attacks."

"Now, many states are emulating our example," Davis said in his January 9 address.

Davis noted that all four of the planes hijacked on September 11th were headed for California, and that more than 100 Californians lost their lives that day.

The governor credited the State Committee on Terrorism he established in 1999 for giving California a "head start in marshaling our forces" for the war on terrorism.

After September 11th, Davis established a state Anti-Terrorism Information Center and appointed as state security advisor George Vinson, a veteran California Highway patrolman who served 23 years with the FBI.

Davis said he is asking the federal government to allow Highway Patrol officers to serve as sky-marshals on in-state flights, and said the state is taking steps to allow law enforcement officials to monitor communications by suspected terrorists and permit "roving" wiretaps on suspects.

Davis also advocated that state employees who are serving in the military reserves National Guard be paid the difference between their military and civilian pay, and urged private sector companies to do the same to "make their Guard employees whole."

KANSAS

In the wake of the terrorist attacks, Kansas has begun development of a central law enforcement data repository that has won the endorsement of the FBI – becoming one of the first states to synchronize its legal and judicial systems with the federal government.

The project, funded in part by a Justice Department grant, relies on PKI technology to authenticate users and control access to information through "crypto cards." The repository was developed in collaboration with Entrust and Verisign to protect FBI files and reduce telecommunication costs.

According to Kansas CIO Don Heiman, the National Association of State Chief Information Officers is promoting the project as a national model.

MICHIGAN

BioPort, the nation's only producer of an anthrax vaccine, has won FDA approval after making several production changes required by federal officials.

Although the vaccine is currently in production, the Lansing, Michigan-based company cannot begin shipping it until a Washington State laboratory that puts the vaccine in vials also wins federal approval.

Hollister-Stier Labs in Spokane, Washington, places the vaccine in vials, and then ships the medication back to Michigan for distribution.

BioPort, which purchased the Lansing laboratory from the state in 1998, has been barred from selling the vaccine since it failed two FDA inspections.

The anthrax vaccine was first licensed by the FDA in the 1970s, but caused controversy when U.S. military troops were sickened after receiving injections in the 1990s. At least one death was blamed on the vaccine.

SOUTH DAKOTA

A bill to prosecute people who threaten terrorist action, even if the threat is a hoax, passed its first legislative hurdle in the state Senate this month.

Endorsing the state's first anti-terrorism legislation, the Senate Judiciary Committee passed a bill that would make it a crime to threaten, inconvenience, or force people to evacuate buildings with bomb threats or threats of violence. The measure

(Continued on page 8)

HDJ PRODUCT PROFILE:

The Rockwell Collins HF Messenger

Rockwell Collins HF Messenger, an advanced High Frequency (HF) Data Communications tool, provides fast, accurate and cost-effective forms of wireless messaging. It permits personal computers or other data input devices to exchange text, files, facsimiles, images and pictures at data rates equivalent to current satellite radios over an HF medium.

The HF Messenger software is used for ground, tactical airborne and maritime HF e-mail applications. It can provide secure data communications through asynchronous or synchronous encryption devices.

Based on a NATO standard (STANAG 5066), HF Messenger provides an unprecedented level of communications interoperability to a wide range of users using disparate communications systems. Currently, members of the US Air Force (SCOPE Command and AWACs), the US Navy (Battle Force E-mail 66), the US Coast Guard, the Department of Health and Human Services, and the U.S. Air Force Auxiliary (Civil Air Patrol), are using HF Messenger for their HF data networks.

HF Messenger provides wireless transmissions between several HF users for broadcast, multicast or point-to-point with services in a Local Area Network (LAN) operating environment. Dedicated point-to-point transmissions between two specific users can also be established. Any LAN-connected users can allocate connections to provide maximum use of HF resources.

HF Messenger provides the required drivers for use with Collins HF radios, and can work with other Automatic Link Establishment radios as well (Motorola, Sunair, Datron). Data Rate Control Algorithms coupled with a HF radio's Automatic Link Maintenance controls the transmission performance to maintain optimum data throughput.

The State of the States: Governors Weigh in On Homeland Security

The Homeland Defense Journal is monitoring statehouses across the nation as governors lay out their agenda and priorities for the upcoming year.

Highlights:

Alabama
Governor Don Siegelman
Proposes to extend to the state National Guard job protections the federal government guarantees every member of the armed services.
Proposes tough penalties, including the death penalty, for those who commit terrorist acts in Alabama.

Arizona
Governor Jane Dee Hull
Proposes the "Arizona Homeland Security Enhancement Act" to prevent money laundering. Establishes a "State Coordinating Council on Homeland Security" to oversee all state response efforts. Activates a call center as part of Operation Vigilance for citizens to call in leads and intelligence information.

Colorado
Governor Bill Owens
Creates the Office of Preparedness and Security within the Department of Public Safety to coordinate planning, response, and training efforts.

New York
Governor George Pataki
Plans initiative to improve airport security.
Asks legislature to pass additional anti-terror measures dealing with those convicted of possessing chemical and biological weapons.
Proposes the Security Through Advanced Research and Technology program to help colleges and universities obtain federal and other research funding for the emerging national homeland security industry. Several NY colleges are working on a uniform of the future that will protect soldiers from injury and detection.

Vermont
Governor Howard Dean
Asks legislature to provide resources to protect the state's computer systems from attack.

West Virginia
Governor Bob Wise
Forms the West Virginia Watch, a volunteer organization of citizens who will assist law enforcement officials in safeguarding people and facilities from attack.

HOMELAND DEFENSE BUSINESS OPPORTUNITIES

Opportunity #1

Project: Nuclear Surety Support Program

Department: Department of Defense

Agency: Defense Threat Reduction Agency

Summary: This program's principle objectives are: (1) provide support to missile defense programs, (2)support capabilities to counter and defeat Weapons of Mass Destruction (WMD) threats, (3) support civil and military response to WMD use, and (4) support the viability and credibility of the nuclear force.

Schedule: Information due January 11, 2002

Value: $8,000,000

Contract Term: 5 years

Contract Type: Indefinite delivery/indefinite quantity

Agency Contact: David Nemerow
(703) 325-6627

Agency Website: http://acquisition.army.mil

Source: FedBizOpps

Source: CBDnet

Opportunity #2

Project: Full Spectrum Information Operations

Department: Department of the Army

Agency: Intelligence and Security Command

Summary: The solicitation is to acquire services to provide continued Information/Warfare Information Operations (IW/IO) support to the land component and separate Army Commanders to facilitate planning and execution of information operations. The prime deliverable of the effort is continued support of automated computer programs, computer models and tools, data bases, decision aids, plans, studies, reports and product development/integration.

Schedule: Questions Due November 26, 2001 Pre-solicitation Conference December 12, 2001 RFP Released February 4, 2002 Est, Award Date August, 5, 2002

Contract Term: 1 base year, 4 option years

Contract Type: Indefinite Delivery Indefinite Quantity

Agency Contact: Lisa Grant
(703) 706-2761

Source: FedBizOpps

Opportunity #3

Project: Systems Engineering and Technical Support

Department: Federal Emergency Management Agency

Agency: Information Technology Services

Summary: The Contractor will be responsible for providing technical assistance for systems engineering, systems design, systems design review, systems integration, and a wide range of project management support activities for the Federal Emergency Management Agency (FEMA) Information Technology Services (ITS) Directorate.

Schedule: Response due February 2, 2002

Competition: 8a

Agency Contact: Linda A. Sudhoff
(202) 646-4672
Gary Fontaine
(202) 646-3356

Agency Website:
http://www.fema.gov/ofm/bidinfo.htm

Source: FedBizOpps

Opportunity #4

Project: Joint Intelligence Virtual Architecture Program

Department: Department of Defense

Agency: Defense Intelligence Agency

Summary: The Joint Intelligence Virtual Architecture (JIVA) program is seeking white papers for a highly integrated Knowledge Discovery (KD) toolkit. Because the desired suite of KD tools does not presently exist as an integrated set, development of the KD toolkit will likely be a technical and functional integration of emerging state of the art components with each other and within the JIVA Enterprise architectural framework.

Schedule: Responses due February 15, 2002

Agency Contact: James Dashiell
(202) 231-2947
jim.dashiell@dia.mil

Source: FedBizOpps

Opportunity #5

Project: Unconventional Nuclear Warfare Protection

Department: Department of Defense

Agency: Defense Threat Reduction Agency

Summary: The Defense Threat Reduction Agency (DTRA) in a joint program effort with the National Nuclear Security Administration (NNSA), is developing a series of test beds to develop and field systems that can defend against threats posed by weapons of mass destruction (WMD), with a priority on nuclear weapons, using unconventional delivery means (e.g., delivery other than by missile or military aircraft). DTRA is currently seeking commercial technology solutions in order to enhance and innovate the Department of Defense's ability to detect, identify, respond, and prevent unconventional nuclear attacks by national, sub-national, or terrorist entities.

Schedule: Responses due January 23, 2002

Agency Contact: Marilyn F. Williams
(703) 325-1193
marilyn.williams@dtra.mil

Agency Website: http://acquisition.army.mil

Source: FedBizOpps

Opportunity #6

Project: Design-Build Construction For Security Engineering And Homeland Defense

Department: Department of the Army

Summary: The work will include construction, renovation, repairs, preventive maintenance, and environmental abatement/improvements for security engineering and homeland defense type projects. The projects will be primarily located in Kansas, Missouri, Nebraska, and Iowa.

Schedule: Proposals Due March 15, 2002

Value: $15,000,000

Competition: Full & Open

Contract Term: 1 year base, 2 option years

Contract Type: Multiple Award Task Order

Agency Contact: Perry Marks
(816) 983-3850
perry.d.marks@usace.army.mil

Source: FedBizOpps

('States' from page 7)

gives judges the authority to force culprits to repay government agencies for damages caused by terrorism or threats of terrorism.

Opponents said the measure could unjustly punish juvenile pranksters who could end up with lifelong criminal records. One lawmaker cited the case of four teenagers prosecuted for exploding fireworks in a portable toilet.

But Assistant Attorney General Charlie McGuigan said such pranks have serious consequences after September 11th, according to an Associated Press report.

"I personally think if you blow up a port-a-potty, that should follow you around awhile," McGuigan said.

VIRGINIA

A Norfolk waste disposal company has contracted with the federal and state environmental agency to burn waste from anthrax decontamination projects.

American Waste Industries began handling the waste in earlier this month after being approached by environmental officials concerned about a growing collection of office furnishings, documents, and uniforms gathered from the anthrax cleanup sites in New York, New Jersey and Washington, D.C.

But the project has been highly controversial in the southern Norfolk neighborhood that houses American Waste Industries' incinerators, where neighbors have deluged officials with concerns about potential health risks, according to the *Virginian-Pilot.*

The controversy erupted after the state Department of Environmental Quality approved the disposal of what it termed "special waste" and alerted the news media.

Officials contend the incineration process is safe because the waste was treated with a chlorine solution before it was shipped.

State regulators determined that any remaining anthrax spores would be killed by temperatures exceeding 300 degrees. American Waste incinerators heat to an average of 1,600 degrees.

According to Frank Daniel of the Virginia Department of Environmental Quality, the incineration process poses "no health risk whatsoever."

The only other facility now disposing of anthrax waste is the U.S. Army's Fort Detrick in Maryland.